EASY SOFTWARE

VERTRAG ÜBER DIE VERARBEITUNG PERSONENBEZOGENER DATEN IM AUFTRAG (AUFTRAGSDATENVERARBEITUNG)

zwischen der EASY SOFTWARE Deutschland GmbH, Am Hauptbahnhof 4, 45468 Mülheim an der Ruhr, (im Folgenden: Auftragnehmer) und dem im Hauptvertrag, der Auftragsbestätigung oder in einem Angebot näher bestimmten Kunden (im Folgenden: Auftraggeber)

Präambel

Dieser „Vertrag über die Verarbeitung personenbezogener Daten im Auftrag“ (nachfolgend Vereinbarung) konkretisiert vor allem die Verpflichtungen der Vertragsparteien zum Datenschutz im Zusammenhang mit dem Umgang des Auftragnehmers mit personenbezogenen Daten des Auftraggebers oder dessen Kunden (nachfolgend Daten). Die datenschutzrechtlichen Regelungen dieser Vereinbarung (§ 1 bis § 8) finden Anwendung auf alle Tätigkeiten bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte, Daten im Auftrage verarbeiten oder mit Daten in Berührung kommen können. Darüber hinaus, werden dem Auftragnehmer im Rahmen des Hauptvertrages oder sonstiger Geschäftsbeziehungen zwischen den Parteien, vertrauliche Informationen aus dem Unternehmen des Auftraggebers zur Verfügung gestellt oder es ist nicht ausgeschlossen, dass der Auftragnehmer in den Geschäftsräumen des Auftraggebers in Kontakt mit solchen Informationen kommt.

§ 1 GEGENSTAND, ART, UMFANG, ZWECK UND DAUER DER AUFTRAGSVERARBEITUNG

1.1. Art, Umfang und Zweck der Datenverarbeitung werden in **Anlage 1** konkretisiert. Der Auftragnehmer darf nur die in Anlage 1 genannten Kategorien an Daten, der dort genannten Betroffenen zu den dort oder in einem eventuell vorhandenen Hauptvertrag genannten Zwecken verarbeiten. Das Vorhandensein eines eventuellen Hauptvertrages wird in der Anlage 1 vermerkt.

1.2. Weitere Konkretisierungen bezüglich Zweck und betroffenen Personen bezüglich abweichender Aufträge werden in zusätzlichen Anhängen zur diesem Vertrag geregelt.

1.3. Jede davon abweichende oder darüberhinausgehende Erhebung oder Verwendung von Daten ist dem Auftragnehmer untersagt, insbesondere eine Verwendung der Daten zu eigenen Zwecken.

1.4. Die Dauer dieser Vereinbarung gilt für die Dauer eines bestehenden Vertragsverhältnisses, insbesondere einem bestehenden Wartungsvertrag, oder einem eventuell vorhandenen Hauptvertrag.

§ 2 VERANTWORTLICHKEIT UND WEISUNGSRECHTE DES AUFTRAGGEBERS

2.1. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Datenschutzbestimmungen im Verhältnis zu Betroffenen und Dritten verantwortlich. Die Verantwortlichkeiten des Auftragnehmers gem. Art. 28 Abs. 10, 82, 83 und 84 der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung, nachfolgend **DSGVO**) bleiben unberührt. Der Auftraggeber ist im Verhältnis der Parteien zueinander Eigentümer der Daten und Inhaber aller Rechte an den Daten.

2.2. Der Auftragnehmer verarbeitet Daten ausschließlich im Auftrag und auf dokumentierte Weisung des Auftraggebers gemäß Art. 28, 29 DSGVO, sofern der Auftragnehmer nicht durch geltendes Recht zu einer Datenverarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber dies vor der Verarbeitung mit, sofern das geltende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.3. Die Weisungen werden anfänglich durch die Anlage 1 und diese Vereinbarung festgelegt und können vom Auftraggeber danach in Textform durch einzelne Weisungen konkretisiert, geändert, ergänzt oder ersetzt werden (Einzelweisung). In dringenden Fällen können Weisungen auch mündlich erteilt werden; eine Bestätigung der Weisung in Textform wird in diesem Fall nachgeholt. Der Auftraggeber besitzt insoweit ein umfassendes Weisungsrecht über Art, Umfang und Zweck der Verarbeitung von Daten.

2.4. Der Auftragnehmer hat Einzelweisungen zumindest in Textform zu bestätigen und zu dokumentieren.

2.5. Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber unverzüglich darüber informieren.

§ 3 PFLICHTEN DES AUFTRAGNEHMERS

3.1. Der Auftragnehmer darf Daten ausschließlich im Rahmen des Auftrages und der Weisungen des Auftraggebers und nur im Gebiet der Europäischen Union (EU) und des Europäischen Wirtschaftsraumes (EWR) verarbeiten. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke als für die der Erfüllung des Hauptvertrages. Der Auftragnehmer darf Daten ohne vorherige Zustimmung in Schriftform durch den Auftraggeber auch nicht an Dritte oder andere Empfänger aushändigen. Hiervon ausgenommen sind Datenweitergaben an Subunternehmer nach Maßgabe von § 6 Abs. (2) zweiter Hs. bleibt unberührt.

3.2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird spätestens zu Beginn der Datenverarbeitung technische und organisatorische Maßnahmen (kurz TOM) gemäß Art 28 Abs. 3 lit. c, Art. 32 in Verbindung mit Art. 5 Abs. 1 und 2 DSGVO zum Schutz der Daten des Auftraggebers treffen und diese für die Dauer dieses Vertrages aufrechterhalten. Dabei ist der aktuelle Stand der Technik unter Berücksich igung des Risikos zu beachten. Diese Maßnahmen werden in **Anlage 3** festgelegt. Eine Änderung der getroffenen Maßnahmen bleibt dem Auftragnehmer nachgelassen, sofern sichergestellt ist, dass das vereinbarte Schutzniveau nicht unterschritten wird. Bei wesentlichen Änderungen wird der Auftraggeber über die Änderungsabsichten des Auftragnehmers rechtzeitig vor deren Umsetzung in Textform informiert. Auf Verlangen weist der Auftragnehmer dem Auftraggeber die Einhaltung dieser Maßnahmen durch Vorlage von Dokumentationsmaterial nach.

3.3. Der Auftragnehmer stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung in seinem Verantwortungsbereich, der etwaige Subunternehmer einschließt, im Einklang mit den Bestimmungen dieser Vereinbarung und den Weisungen des Auftraggebers erfolgt und die technisch-organisatorischen Maßnahmen eingehalten werden. Der Auftragnehmer ist verpflichtet, die Kontrollen zu dokumentieren und dem Auftraggeber diese auf Verlangen vorzulegen.

3.4. Der Auftragnehmer hat, sofern nicht bereits geschehen, alle mit der Verarbeitung der Daten beschäftigten Personen schriftlich zur Verschwiegenheit gem. DSGVO zu verpflichten, soweit diese Personen nicht bereits einer vergleichbaren, auch gesetzlichen, Verschwiegenheitspflicht unterliegen. Der Auftragnehmer hat diese Personen dabei in die wesentlichen gesetzlichen Bestimmungen über den Datenschutz einzuweisen und sie zu verpflichten, diese Bestimmungen zu beachten. Auf Verlangen des Auftraggebers wird der Auftragnehmer dies durch Vorlage der Verpflichtungserklärungen nachweisen.

3.5. Der Auftragnehmer gewährleistet, einen Datenschutzbeauftragten zu bestellen und zumindest während der Dauer dieser Vereinbarung zu beschäftigen. Der Name des Datenschutzbeauftragten sowie die Kontaktdaten können der Datenschutzerklärung auf der Homepage des Auftragnehmers (www.easy.de) entnommen werden.

3.6. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten des Auftraggebers aus Art. 32 DSGVO (TOM), aus Art. 33 und 34 DSGVO (Meldeverpflichtungen bei Datenpannen) und ggf. aus Art. 35 DSGVO (Datenschutz-Folgenabschätzung) sowie Art. 36 DSGVO (Konsultation der Aufsichtsbehörde).

3.7. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

§ 4 ANFRAGEN BETROFFENER

4.1. Für den Fall, dass ein Betroffener gegenüber dem Auftraggeber berechtigte datenschutzrechtliche Ansprüche geltend macht, wird der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, der Erfüllung dieser Ansprüche nachzukommen.

4.2. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Geltendmachung seiner Rechte wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer wird insbesondere keine Auskunftsverlangen Betroffener beantworten.

§ 5 KONTROLLRECHTE DES AUFTRAGGEBERS

5.1. Der Auftraggeber ist berechtigt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von der Einhaltung der technischen und organisatorischen Maßnahmen durch den Auftragnehmer zu überzeugen. Der Auftraggeber dokumentiert das Ergebnis dieser Kontrollen. Hierfür kann der Auftraggeber z.B. Auskünfte des Auftragnehmers einholen oder zu den üblichen Geschäftszeiten vor Ort in den Geschäftsräumen des Auftragnehmers prüfen oder durch einen Dritten prüfen lassen.

5.2. Der Auftragnehmer gewährt dem Auftraggeber oder einem von ihm beauftragten Dritten die zur Durchführung der Kontrollen erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte und wirkt bei der Kontrolle in angemessenem Umfang aktiv mit.

§ 6 UNTERAUFTRAGSVERHÄLTNISSE („SUBUNTERNEHMER“)

6.1. Der Auftragnehmer darf geeignete Subunternehmer im Gebiet der EU oder des EWR mit der Verarbeitung von Daten im Auftrag und nach Weisung betrauen, wenn der Auftraggeber dem im Einzelfall schriftlich vor Beauftragung des Subunternehmers zugestimmt hat. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder den Austausch von Subunternehmer informieren. Der Auftraggeber kann der Hinzuziehung oder dem Austausch von Subunternehmern nach Information durch den Auftragnehmer widersprechen. Ein Widerspruch darf nur aus wichtigem Grund erfolgen.

6.2. Dem Subunternehmer müssen die gleichen Datenschutzpflichten auferlegt werden, die in diesem Vertrag festgelegt sind. Insbesondere ist sicherzustellen, dass die geeigneten technischen und organisatorischen Maßnahmen vom Subunternehmer so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Datenschutzrechts erfolgt. Dem Auftraggeber sind in dem Subunternehmervertrag gegenüber dem Subunternehmer unmittelbar sämtliche Kontrollrechte gem. §5 im Sinne eines echten Vertrages zugunsten Dritter einzuräumen.

6.3. Der Auftraggeber kann den Auftragnehmer dazu auffordern, Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers zu erteilen und Einsicht in die relevanten Vertragsunterlagen zu gewähren.

6.4. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Subunternehmers.

6.5. Die in der **Anlage 2** aufgelisteten Subunternehmer gelten als genehmigt.

6.6. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§ 7 BESONDERE PFLICHTEN DES AUFTRAGNEHMERS BEI „DATENPANNEN“

7.1. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen datenschutzrechtliche Vorschriften oder diese Vereinbarung, wenn Anhaltspunkte dafür bestehen, dass Daten unrechtmäßig verarbeitet worden sind. § 3 Abs. (7) bleibt unberührt. Der Auftragnehmer trifft außerdem die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen.

7.2. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

§ 8 RÜCKGABE BZW. LÖSCHUNG VON DATENTRÄGERN BZW. DATEN

8.1. Der Auftragnehmer berichtigt, löscht oder sperrt die Daten unverzüglich, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Löschung von Daten bzw. Vernichtung von Datenträgern übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern dies nicht bereits einem eventuellen Hauptvertrag vereinbart ist. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung zur Löschung nicht erforderlich. Gesetzliche Aufbewahrungsverpflichtungen bleiben unberührt.

8.2. Der Auftragnehmer hat Daten nach Vertragsbeendigung nach Wahl des Auftraggebers zu löschen und/oder zurückzugeben, es sei denn, der Auftragnehmer ist zu einer Speicherung aufgrund anderer Vorschriften verpflichtet. Der Auftragnehmer hat an den Daten kein Zurückbehaltungsrecht, es sei denn, sein Gegenanspruch ist rechtskräftig festgestellt oder unbestritten.

§ 9 SCHRIFTFORMKLAUSEL, VERHÄLTNIS ZUM HAUPTVERTRAG, RECHTSWAHL

9.1. Änderungen und Ergänzungen dieser Vereinbarung bedürfen einer schriftlichen Vereinbarung. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.2. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung den Regelungen eines eventuell bestehenden Hauptvertrages vor.

9.3. Es gilt deutsches Recht.

ANLAGE 1

ZWECK, ART UND UMFANG DER DATENVERARBEITUNG, ART DER DATEN UND KREIS DER BETROFFENEN

- Installation von Software beim Auftraggeber
- Wartung und Support der Installation bei Auftraggeber
- Fernwartung der Installation beim Auftraggeber

ART UND UMFANG DER VERARBEITUNG

- Zugriff auf Daten im Wege des Remote-Zugriffs
- Zwischenspeicherungen beim Remote-Zugriff
- Anzeigenlassen von Daten im Wege des Remote-Zugriffs
- Aufnahme der Störungen des Auftraggebers in einem Ticketsystem
- Führung einer Projektakte bezüglich der Installation des Auftraggebers.
- Zugriff des Auftraggebers auf das Extranet zur Information.

ART DER DATEN

- Vor- und Zunamen
- Geburtsdaten
- Anschriften
- E-Mail-Adressen
- Telefonnummern
- IP-Adressen
- Personalakten

KREIS DER BETROFFENEN

- Kunden des Auftraggebers
- Mitarbeiter des Auftraggebers
- Potentielle Kunden des Auftraggebers und Interessenten
- Lieferanten des Auftraggebers

ANLAGE 2

IM VORAUS GENEHMIGTE UNTERAUFTRAGNEHMER

- EASY SOFTWARE AG, Am Hauptbahnhof 4, 45468 Mülheim an der Ruhr
- OTRIS Software AG in Dortmund, Königswall 21, 44137 Dortmund
- CTO Balzuweit GmbH, Lautlinger Weg 3, 70567 Stuttgart
- I.R.I.S. AG, Heusstraße 23, 52078 Aachen
- Contellix GmbH, Mainzer Landstraße 41, 60329 Frankfurt
- friendWorks GmbH, Theresienplatz 31, 94315 Straubing
- SAP Deutschland SE & Co.KG, Rosenthaler Straße 30, 10178 Berlin

ANLAGE 3

TECHNISCH ORGANISATORISCHE MAßNAHMEN

VERTRAULICHKEIT
(d.h. Daten sind für Unberechtigte nicht zugänglich)

RICHTLINIEN:
- Anhand von Datenschutzrichtlinien ist geregelt, wie mit personenbezogenen Daten im konkreten Fall umzugehen ist.
- Im Rahmen der IT-Sicherheitsrichtlinien ist der sichere Umgang mit Soft- und Hardware definiert sowie die einzuhaltenden Sicherheitsmaßnahmen

SCHULUNG:
- Beschäftigte erhalten regelmäßig Schulungen zum Datenschutz und zur Informationssicherheit.

ZUTRITTSKONTROLLE:
(verhindert, dass Unbefugte räumlich Zutritt zu den Verarbeitungsanlagen/-räumen personenbezogener Daten oder sonstigen personenbezogenen Unterlagen, z. B. Akten oder Datenträgern erhalten)

- Die Zutrittskontrolle zu den Gebäuden oder externen Büros wird entweder über Karten oder aber über Schlüssel gewährt.
- Karten sind mit einem Bild versehen ohne die Nennung des Firmennamens.
- Der Zugang zum internen Rechenzentrum ist mit einer zusätzlichen Sicherung versehen. Nur Mitarbeiter mit dem entsprechenden Recht dürfen diesen Bereich betreten.
- Das firmeneigene Rechenzentrum befindet sich in der Hauptstelle in Mülheim. Dieses Gebäude ist mit einer Alarmanlage gesichert die direkt mit einem Sicherheitsdienst gekoppelt ist. Im Laufe des Jahres 2018 verlagern wir unser IT in ein externes Rechenzentrum mit ISO 27001 Zertifizierung
- Bei externen Rechenzentren achten wir auf eine ISO 27001 Zertifizierung und effektive Maßnahmen zur Zutrittskontrolle
- Besucher der Hauptstelle müssen sich anmelden und bekommen einen Besucherausweis. In den Außenstellen müssen diese sich bei einem Mitarbeiter melden, so dass eine Kontrolle stattfindet. Gemäß IT-Sicherheitsrichtlinie dürfen sich Besucher nicht unbegleitet im Gebäude aufhalten.
- Sensible Datenträger und Papierakten werden in abschließbaren Schränken aufbewahrt.

ZUGANGSKONTROLLE / BENUTZERKONTROLLE:
(verhindert, dass Unbefugte die DV-Systeme in denen personenbezogene Daten verarbeitet werden nutzen können, z. B. User/Passwort-Regelung)

- Der Zugriff auf DV-Anwendungen erfordert eine personalisierte Anmeldung mit dedizierten Benutzerrechten.
- Passwörter müssen eine Länge von 12 Zeichen haben und sollen Groß- und Kleinbuchstaben sowie Zahlen beinhalten.
- Die Speicherung von Passwörtern erfolgt gehasht.
- Die Anzahl der Anmeldeversuche an der Domäne ist begrenzt.
- Nicht mehr genutzte Benutzerkonten werden umgehend deaktiviert.
- Ein Zugriff auf Unternehmensressourcen ohne eine Authentifizierung ist nicht möglich.

ZUGRIFFSKONTROLLE / SPEICHERKONTROLLE / DATENTRÄGERKONTROLLE:
(gewährleistet, dass Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten und Funktionen zugreifen können, z. B. durch Rollen-/Berechtigungskonzepte)

- Als Basis für die Rechtevergabe wird ein Active Directory von Microsoft verwendet. Hier werden über Gruppenzuordnungen die Rechte auf die einzelnen Ressourcen des Netzes vergeben. Wenn möglich werden andere Softwareprodukte an das AD gekoppelt. In der Regel bieten alle eingesetzten Produkte die Möglichkeit der Unterscheidung der Rechte nach Erstellen, Lesen, Schreiben und Löschen.
- Rechte an Ressourcen werden nur nach Notwendigkeit vergeben.
- Rechte müssen über das Ticketsystem des internen IT-Support angefordert werden. Diese werden nur nach Bestätigung durch den entsprechenden Vorgesetzten vergeben.
- Alle Datenträger werden gemäß IT-Sicherheitsrichtlinie verschlüsselt. Durch Löschen der entsprechenden Key werden die Daten auch auf SSD Datenträgern sicher gelöscht. Bei Veräußerung oder Außerbetriebnahme werden Datenträger noch einmal gelöscht.
- Zur Vernichtung von Papierunterlagen stehen Papierschredder zur Verfügung. Bei größeren Mengen wird zu Vernichtung ein Container eines entsprechend zertifizierten Dienstleisters angefordert.

TRENNUNGSGEBOT / TRENNBARKEIT:
(gewährleistet, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können, z. B. durch System- oder Mandantentrennung, etc.)

- Die Daten verschiedener Auftraggeber werden durch Vergabe von Berechtigungen logisch getrennt und sind dementsprechende auch getrennt löschbar sowie einsehbar.
- Es werden nur mandantenfähige oder Systeme mit logischer Trennbarkeit eingesetzt.

AUFTRAGSKONTROLLE:
(gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können)

- Die Erhebung, Verarbeitung, Berichtigung und Löschung der Daten erfolgt streng gebunden an Auftrag und Einzelweisungen des Auftraggebers gemäß der hier getroffenen vertraglichen Vereinbarungen.
- Unterauftragnehmer werden unter besonderer Berücksichtigung von § 11 BDSG bzw. Art. 28 DSGVO und somit der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt.
- Aufträge und damit verbundene Auftrags(daten)verarbeitungsvereinbarungen werden schrif lich erteilt.
- Verträge mit Unterauftragnehmern in Drittstaaten werden unter Anwendung der EU-Standardvertragsklauseln abgeschlossen.
- Beschäftigte sowie eingesetzte Unterauftragnehmer, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, sind schriftlich auf das Datengeheimnis bzw. zur Vertraulichkeit verpflichtet.

VERSCHLÜSSELUNG:
(gewährleistet, dass auf besonders sensible personenbezogene Daten nur mit Kenntnis eines spezifischen Entschlüsselungscodes zugegriffen werden kann)

- Notebooks, Smartphones, USB Sticks und sonstige mobile Datenträger auf denen sich Daten des Auftraggebers befinden, sind verschlüsselt. Dazu verwenden wir Bitlocker unter Windows oder Filevault unter MacOsX.
- Für die Erstellung von verschlüsselten Containern verwenden wir die OpenSource Applika ion Veracrypt. Dies kann von jedem MA bei Bedarf installiert werden.
- Bei der Verwendung von Webapplika ionen, sorgen wir für die ausschließliche Ansprechbarkeit über HTTPS.
- Wir stellen den MA ein VPN zur Verfügung, damit diese bei außer Haus Einsätzen eine sichere Netzwerkverbindung nutzen können.

EASY SOFTWARE

ANONYMISIERUNG / PSEUDONYMISIERUNG:
(gewährleistet, dass die Identifikation einer bestimmten Person vermieden bzw. erschwert wird, sofern eine Identifikation dieser Person für den Zweck der Verarbeitung der personenbezogenen Daten nicht zwingend erforderlich ist – „Datenvermeidung“.)

- Wo immer sinnvoll und möglich (z. B. für Statistiken) werden personenbezogene Daten pseudonymisiert oder anonymisiert.

INTEGRITÄT
(d.h. Daten können nicht verfälscht werden)

TRANSPORTKONTROLLE / ÜBERTRAGUNGSKONTROLLE (WEITERGABEKONTROLLE):
(gewährleistet, dass personenbezogene Daten bei der Weitergabe, also Übertragung oder ihres Transports nicht unbefugt gelesen, kopiert verändert oder entfernt werden können, z. B. durch Transportverschlüsselung)

- Der Zugriff auf Web-basierte DV-Systeme in denen personenbezogene Daten verarbeitet werden ist nur über verschlüsselte Kommunikationsverbindungen (https und TLS) möglich.
- Der Fernzugriff auf das interne IT-Netzwerk von IT-Systemen außerhalb des hausinternen Netzes erfolgt ausschließlich mittels VPN-Technologie.
- Der ein- und ausgehende Datenverkehr wird mittels einer Firewallapliance überwacht. Zeitpunkt, Inhalt, Empfänger sowie der veranlassende Sender von Datenübertragungen werden protokolliert.
- Beim physischen Transport personenbezogener Daten werden sichere Transportbehälter/-verpackungen eingesetzt. Transportpersonal und –fahrzeuge (z. B. bei Kurierdiensten) werden sorgfältig ausgewählt.
- Zum Transport verwendete Datenträger müssen verschlüsselt werden.

EINGABEKONTROLLE:
(gewährleistet, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind, . B. durch Protokollierung)

- Eingaben in und Veränderungen an relevanten Anwendungssystemen werden mittels Protokollen/Logfiles aufgezeichnet und überwacht. Dabei sind die Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten (Inhalt und Zeitpunkt der Änderung) sowie der Ausführende (durch individuelle Benutzernamen, nicht Benutzergruppen) gewährleistet.

VERFÜGBARKEIT, BELASTBARKEIT / WIDERSTANDSFÄHIGKEIT, WIEDERHERSTELLBARKEIT
(d.h. Daten stehen zur Verfügung, wenn sie gebraucht werden)

VERFÜGBARKEITSKONTROLLE:
(gewährleistet, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind, z. B. durch Brandschutzmaßnahmen, etc.)

- Die Server sind über eine USV gegen Stromausfall abgesichert.
- Wir verwenden Virtualisierungslösungen für Server, so dass bei Ausfall einzelner Maschinen ein Weiterbetrieb auf einer anderen Instanz möglich ist.
- Die Serverräume sind klima isiert.
- Es kommen moderne Brandschutz- und -meldeanlagen zum Einsatz. Automatische Gaslöschanlagen verhindern weitergehende Schäden.

BELASTBARKEIT (IM SINNE VON: WIDERSTANDSFÄHIGKEIT):
(gewährleistet, dass die IT-Systeme widerstandsfähig gegen Angriffe sind)

- Alle DV-Systeme auf denen die vereinbarten Services laufen, sind durch eine Firewall vor Zugriffen von außen geschützt.
- Updates müssen bei Verfügbarkeit zeitnah in alle Systeme eingespielt werden. Automatische Updatemechanismen sind bevorzugt.
- Alle Systeme sind mit Anti-Viren-Software ausgestattet.
- Einsatz von Intrusion-Detection-Systemen in der zentralen Firewall.
- Das Antwortzeitverhalten wesentlicher Systeme wird regelmäßig überwacht, um außergewöhnliche Belastungssituationen (z. B. durch Cyberangriffe) und damit einen möglichen Ausfall der Systeme frühzeitig identifizieren zu können.

WIEDERHERSTELLBARKEIT:
(gewährleistet, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können)

- Die regelmäßig in verschiedenen Generationen automatisch erzeugten Datensicherungen werden redundant in verschiedenen Gebäudeteilen verwahrt.

SICHERSTELLUNG DER DAUERHAFTEN WIRKSAMKEIT DER GETROFFENEN MAßNAHMEN:
(gewährleistet, dass getroffene Maßnahmen regelmäßig überprüft und bei Bedarf angepasst werden)

- Die ordnungsgemäße Einhaltung und Durchführung der hier aufgeführten Maßnahmen wird manuell und/oder DV-technisch protokolliert (Nachweispflicht).
- Alle hier aufgeführten Maßnahmen unterliegen einem regelmäßigen Review und werden kontinuierlich verbessert.